(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 237 071 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.09.2002 Bulletin 2002/36

(51) Int Cl.[7]: **G06F 7/58**

(21) Application number: **01105024.2**

(22) Date of filing: **01.03.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.**
Kadoma-shi, Osaka 571-8501 (JP)

(72) Inventors:
- **Räth, Detlef**
  31234 Edemissen (DE)
- **Kelb, Frank**
  31224 Peine (DE)
- **Trotzke, Hendrik**
  31241 Ilsede (DE)

(74) Representative:
Lins, Edgar, Dipl.-Phys. Dr.jur. et al
Gramm, Lins & Partner GbR,
Theodor-Heuss-Strasse 1
38122 Braunschweig (DE)

(54) Method for generating a random number and electronic apparatus having a memory for storing a random number

(57) For generating a true random number (9) in an electronic apparatus without using expensive components the following steps are performed:

- determining the time of an externally initiated event within the apparatus which externally initiated event not being synchronised to any signal within the apparatus,
- determining the state of a periodic signal (1) within the apparatus in relation to the time of said externally initiated event, and
- transforming said determined state of said periodic signal (1) into a digital amount, being the random number (10).

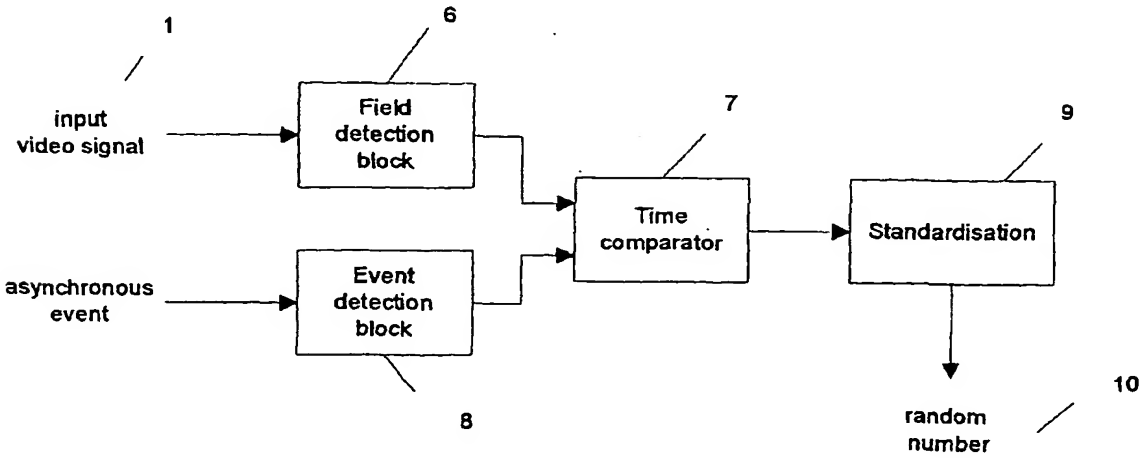

Fig.2

EP 1 237 071 A1

Description

[0001] The invention relates to a method for generating a random number in an electronic apparatus.

[0002] Furthermore, the invention relates to an electronic apparatus having a memory for storing a random number and including a stage for processing a synchronic signal and a generator for a predetermined signal not synchronised with said synchronic signal upon an external action.

[0003] Electronic apparatus suited for processing electronic data regularly include a memory for storing a random number which is e.g. used as an identification number of the apparatus. In order to establish a sufficient safety against finding the random number by trials in order to misuse the apparatus the random number has to be chosen from a sufficient large amount of potential numbers.

[0004] The statistic safety obtained thereby is, however, only obtained if the random number is a true random number so that the number is in no way predictable.

[0005] Known methods of generating random numbers have proved to be not truly random, i.e. the numbers are predictable maybe by means of a pretty complicated algorithm. A further disadvantage of known methods is caused by more or less expensive additional means for generating the random number.

[0006] It is an object of the present invention to allow the generation of a true random number with little expenses.

[0007] According to the present invention this object is achieved by a method for generating a random number in an electronic apparatus comprising the steps of

- determining the time of an externally initiated event within the apparatus which externally initiated event not being synchronised to any signal within the apparatus,
- determining the state of a periodic signal within the apparatus in relation to the time of said externally initiated event, and
- transforming said determined state of said periodic signal into a digital amount being the random number.

[0008] According to the present invention a periodic signal processed within the apparatus is put in relation to an externally initiated event by which a predetermined signal, like a pulse, is produced within the apparatus. Care must be taken that the predetermined signal is not synchronised with the periodic signal, in order to guarantee the random number to be not predictable.

[0009] For avoiding any unintentional synchronisation of the externally initiated signal with the periodic signal a signal generated outside the apparatus and received by said apparatus from outside may be used as the periodic signal the state of which being determined. This can easily be achieved if the apparatus is a video signal receiving apparatus and a video signal is used as said periodic signal. Most preferably synchronous pulses, preferably fields synchronous pulses of the video signals may be used as the periodic signal.

[0010] The above-mentioned object of the invention may also be achieved by an electronic apparatus having a memory for storing a random number and including a stage for processing a synchronic signal and a generator for a predetermined signal not synchronised with that synchronic signal upon an external action which is characterised in that a control determines the time of the occurrence of said predetermined signal, determines the state of said periodic signal in relation to said determined time, obtaining said determined state of said periodic signal in digitised form as the random number and transfers said random number into the memory.

[0011] In a preferred embodiment of the invention a time period between the occurrence of said externally initiated event and a periodic state of the periodic signal is determined and digitised into said digital amount. This method can be achieved in an apparatus wherein the control starts a counter upon occurrence of the predetermined signals and stops said counter upon detection of the periodic state of the periodic signal. Thereby the random number is not only not predictable but there is also the same probability for choosing a number out of all potential numbers.

[0012] In a further embodiment of the present invention an amplitude of the periodic signal is digitised into said digital amount at the time of the occurrence of said externally initiated event. This can be done by a control which comprises a sensing element to sensing the amplitude of the periodic signal and switches the output signal of the sensing element upon occurrence of said predetermined signal to an a-d-converter the output of which is connected to the memory for the random number.

[0013] In still a further embodiment of the present invention a counter of a timer counting periodically is interrupted by the externally initiated event and the state of the interrupted counter is used as the random number.

[0014] The present invention, its advantages and advantagous aspects will be more fully understood by the detailed description of a preferred embodiment with reference to the accompany drawings, wherein

Fig. 1 shows an example for a periodic video signal and an asynchronous event producing an asynchronous pulse, and

Fig. 2 shows a schematic block diagram of the parts of an electronic apparatus relevant for performing the present invention.

[0015] Figure 1 shows a video signal 1 having a periodic length T which is in the present case defined by (vertical) field sync pulses starting a block 2 wherein the content of a vertical video frame is contained. After a vertical blanking gap 3 the next field is started by a field sync pulse. To an arbitrary time an asynchronous event is initiated within the apparatus, e.g. by pressing a key of the apparatus, e.g. for switching the apparatus on into an active state. By said event a predetermined signal in form of a rectangular pulse 4 is produced. Within the apparatus the time period delta T 5 between the falling flank of the pulse 4 and the start of the next field block 2 is determined and in digital form used as the random number.

[0016] For working according the method of figure 1 an apparatus indicated in figure 2 is used. The input video signal 1 is processed in a field detection block 6 wherein the beginning of the field 2 is detected and characterised by an output pulse inputted to one input of a time comparator 7.

[0017] An asynchronous event, e.g. the pressing of a key of the apparatus is detected by an event detection block 8 outputting pulse 4 to a second input of time comparator. Time comparator 7 compares the period of time delta T 5 between both input pulses and outputs said delta T 5 to a standardisation circle 9 which produces a digital number corresponding to delta T 5 and outputs the digital number as random number 10 to a (not shown) memory for said random number 9.

[0018] By this way random number 10 may be generated and transmitted to memory for random number 10 by using components and stages of the electronic apparatus which usually exist within said apparatus so that additional components and stages are not necessary. Therefore, random number 10 may be generate in a simple and cheap way.

Claims

1. Method for generating a random number (9) in an electronic apparatus, comprising the steps of

   - determining the time of an externally initiated event within the apparatus which externally initiated event not being synchronised to any signal within the apparatus,
   - determining the state of a periodic signal (1) within the apparatus in relation to the time of said externally initiated event, and
   - transforming said determined state of said periodic signal (1) into a digital amount, being the random number (10).

2. Method according to claim 1, wherein the periodic signal (1), the state of which being determined, is a signal generated outside the apparatus and received by said apparatus from outside.

3. Method according to claim 2, wherein said apparatus is a video signal receiving apparatus and a video signal is used as said periodic signal (1).

4. Method according to claim 3, wherein synchronous pulses of said video signal are used as said periodic signal (1).

5. Method according to claim 4, wherein field synchronous pulses are used as said periodic signal (1).

6. Method according to one of the claims 1 to 5, wherein a time period delta T (5) between the occurrence of said externally initiated event and a periodic state of said periodic signal (1) is determined and digitised into said digital amount.

7. Method according to claim 6, wherein a counter is started by said externally initiated event and stopped by said periodic state of said periodic signal (1).

8. Method according to one of the claims 1 to 5, wherein an amplitude of the periodic signal (1) at the time of the occurrence of said externally initiated event is digitised into said digital amount.

9. Method according to claim 8, wherein the amplitude is digitised by an a-d-converter.

10. Method according to one of the claims 1 to 5, wherein a counter of a timer counting periodically is interrupted by said externally initiated event and the state of the interrupted counter is used as the random number (10).

11. Electronic apparatus having a memory for storing a random number (9) and including a stage for processing a synchronic signal (1) and a generator (8) for a predetermined signal (4) not synchronised with said synchronic signal (1) upon an external action, **characterised in that** a control determines the time of the occurrence of said predetermined signal (4) determents the state of said periodic signal (1) in relation to said determined time, obtaining said determined state of said periodic signal (1) in digitised form as said random number (10) and transfers the random number (9) into the memory.

12. Electronic apparatus according to claim 10, **characterised in that** the control starts a counter upon occurrence of the predetermined signal (4) and stops said counter upon detection of a periodic state of the periodic signal (1).

13. Electronic apparatus according to claim 11, **characterised in that** the control comprises a sensing element sensing the amplitude of the periodic signal (1), and switches the output signal of the sensing element upon occurrence of said predetermined signal (4) to an a-d-converter the output of which is connected to the memory for the random number (10).

14. Electronic apparatus according to claim 11, **characterised in that** the control interrupts a counter of a timer counter periodically upon occurrence of said predetermined signal (4) and that the state of interrupted counter can be outputted to the memory for the random number (10).

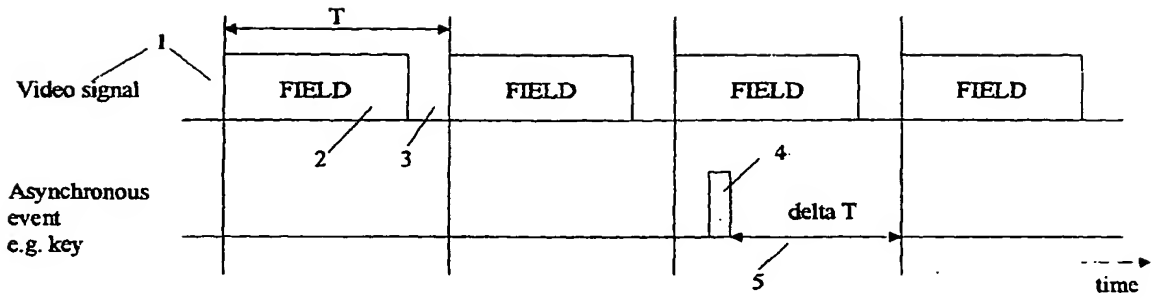
T
1
Video signal
FIELD
FIELD
FIELD
FIELD
2
3
4
Asynchronous
event
e.g. key
delta T
5
time

Fig.1

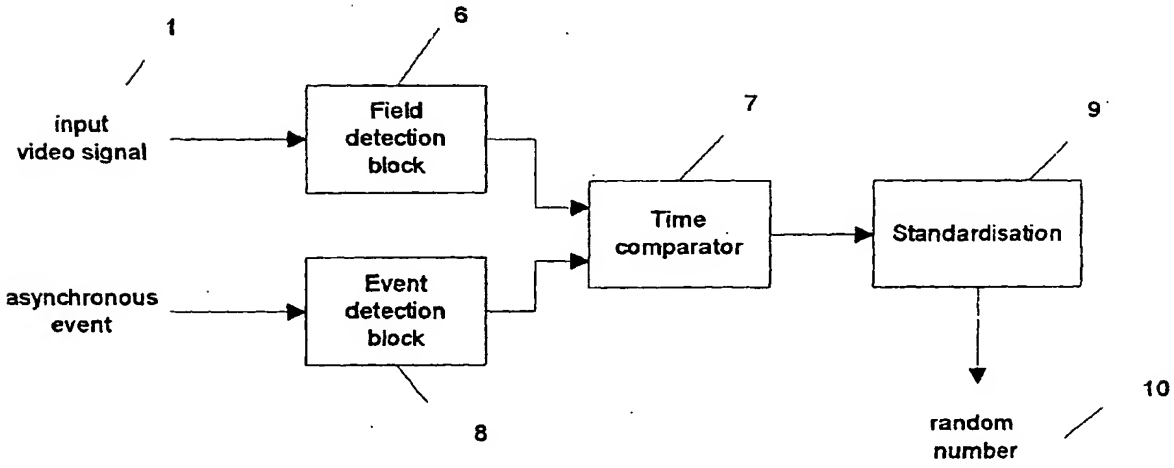
1
6
input
video signal
Field
detection
block
7
9
Time
comparator
Standardisation
asynchronous
event
Event
detection
block
8
10
random
number

Fig.2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 10 5024

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X A	EP 0 449 265 A (GAO GES AUTOMATION ORG) 2 October 1991 (1991-10-02) * column 3, line 30 - line 51 *	1-5,10, 11,14 6-9,12, 13	G06F7/58
A	US 6 076 097 A (XIAO SIHAI ET AL) 13 June 2000 (2000-06-13) * abstract *	6-8,12	
A	EP 0 365 930 A (IBM) 2 May 1990 (1990-05-02) * abstract *	1-14	
A	EP 0 011 050 A (GRETAG AG) 14 May 1980 (1980-05-14) * page 3, last paragraph *	1-14	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	17 August 2001	Cohen, B

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 10 5024

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

17-08-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0449265 A	02-10-1991	DE 4010305 A	02-10-1991
		AT 153815 T	15-06-1997
		DE 59108715 D	03-07-1997
		ES 2101701 T	16-07-1997
		JP 7311673 A	28-11-1995
		US 5627894 A	06-05-1997
US 6076097 A	13-06-2000	NONE	
EP 0365930 A	02-05-1990	US 4905176 A	27-02-1990
		JP 1926190 C	25-04-1995
		JP 2128218 A	16-05-1990
		JP 6058623 B	03-08-1994
EP 0011050 A	14-05-1980	AT 837 T	15-04-1982
		CA 1138069 A	21-12-1982
		DE 2962468 D	19-05-1982
		JP 55061839 A	09-05-1980
		US 4313031 A	26-01-1982

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82